US-CERT National Cyber Alert System

SB04-245-Summary of Security Items from August 18 through August 31, 2004

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends and viruses identified between August 18 and August 31, 2004. **Updates to items appearing in previous bulletins are listed bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - altSoft aGSM Half-Life Server Info Response Buffer Overflow
  - Bird Chat Remote Denial of Service
  - Cisco Secure Access Control Server Multiple Remote Vulnerabilities
  - EFS Software Easy File Sharing Web Server Information Disclosure & Remote Denial of Service
  - Gadu-Gadu Spoofed File Extension
  - IpSwitch WhatsUp Gold Remote Buffer Overflow
  - Keene Software Keene Digital Media Server Directory Traversal
  - Massive Entertainment Ground Control II Remote Denial of Service
  - Merak Mail Server Webmail Multiple Vulnerabilities
  - Microsoft Internet Explorer Resource Detection
  - Microsoft Internet Explorer Drag & Drop File Installation
  - Microsoft Internet Explorer MHTML Content-Location Cross Security Domain Scripting
  - Microsoft NTP Time Synchronization Spoof
  - NakedSoft Gaucho POP3 Email Header Buffer Overflow
  - Niho Software Inc. Web Log Analyzer Cross-Site Scripting
  - Nullsoft Winamp Skin File Remote Code Execution
  - Pedestal Software Integrity Protection Driver Local Denial of Service
  - People Can Fly Painkiller Remote Buffer Overflow
  - RealVNC Server Remote Denial of Service
  - Sysinternals Regmon Local Denial of Service
  - Webroot Window Washer Erased Files
  - Working Resources, Inc. BadBlue Webserver Denial of Service
  - ZoneAlarm/ZoneAlarm Pro Weak Default Permissions
- UNIX / Linux Operating Systems
  - **Adobe Acrobat Reader Shell Command Injection and Buffer Overflow Vulnerability (Updated)**
  - Anton Raharja PlaySMS SQL Input Validation
  - Apple Mac OS X Safari 'Show in Finder
  - Ben Yacoub Hatem MySQL Backup Pro Information Disclosure
  - Bharat Mediratta Gallery Input Validation
  - British National Corpus SARA Remote Buffer Overflow
  - Double Precision, Inc.Courier-IMAP Remote Format String
  - EnderUNIX SDT Hafiye Terminal Escape Sequence
  - FIDOGATE Input Validation
  - **Gaim Buffer Overflows in Processing MSN Protocol (Updated)**
  - GNU a2ps Command Injection
  - Hitachi Job Management Partner 1 Authentication Flaw & Remote Denial of Service
  - IMWheel Insure File Creation
  - InfoTecna s.r.l. SERCD, SREDIRD Format String & Buffer Overflow
  - INL Ulog-php Input Validation
  - Inter7 Vpopmail Vsybase.c Multiple Vulnerabilities
  - Inter7 Vpopmail SQL Injection
  - John Bradley XV Multiple Buffer Overflow and Integer Handling
  - **Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory to Local Users (Updated)**
  - Marc Lehmann RXVT-Unicode Open File Descriptor Leakage
  - Multiple Vendor Zlib Compression Library Remote Denial of Service
  - Multiple Vendor GLibC LD_DEBUG Information Disclosure
  - Multiple Vendor Qt Image File Buffer Overflows
  - Multiple Vendor KDE Konqueror Cookie Domain Validation
  - Multiple Vendor KDE Insecure Temporary Directory Symlink
  - Multiple Vendor KDE DCOPServer Insecure Temporary File Creation
  - **Multiple Vendor Konqueror Frame Injection Vulnerability (Updated)**
  - Multiple Vendor Linux Kernel Race Condition
  - multiple Vendor TNFTPD Multiple Signal Handler Remote Privilege Escalation
  - Multiple Vendor Mozilla/Netscape/Firefox Browsers Content Spoofing
  - Music Daemon Information Disclosure
  - MySQL Mysql_real_connect Function Remote Buffer Overflow
  - MySQL 'Mysqlhotcopy' Script Elevated Privileges
  - OpenBSD Bridged Network ICMP Denial of Service
  - **OpenBSD isakmpd Multiple Unspecified Remote (Updated)**
  - PHP Code Snippet Library Multiple Cross-Site Scripting
  - RaXnet Cacti Auth_Login.PHP Authentication Bypass
  - **GNOME VFS updates address exists vulnerability (Updated)**
  - Rob Flynn Gaim Multiple Vulnerabilities
  - **Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or Write Arbitrary Files (Updated)**
  - Samba Remote Print Change Notify Remote Denial of Service
  - **SoX ".WAV" File Processing Buffer Overflow Vulnerabilities (Updated)**
  - SpamAssassin Remote Denial of Service
  - Sun Microsystems, Inc. Sun CDE Mailer Buffer Overflow
  - Sun Microsystems, Inc. CDE LibDTHelp LOGNAME Environment Variable Buffer Overflow
  - SUPHP Elevated Privileges
  - SWSoft Plesk 'Login_name' Parameter Cross-Site Scripting
  - Sympa List Creation Authentication Bypass
  - Sympa Cross-Site Scripting
  - WebAPP Directory Traversal
  - **Xine Project xine Buffer Overflow in Processing 'vcd' Identifiers Lets Remote Users Execute Arbitrary Code (Updated)**
  - Yukihiro Matsumoto Ruby CGI Session Management Unsafe Temporary File
- Multiple Operating Systems
  - AWStats 'awstats.pl' Input Validation
  - Axis Communications Axis Network Camera And Video Server Multiple Vulnerabilities
  - Axis Communications StorPoint CD Administrative Backdoor
  - Cisco Systems IOS OSPF Remote Denial of Service
  - Cisco Systems IOS Telnet Service Remote Denial of Service
  - Dynix WebPAC Input Validation
  - EGroupWare Multiple Input Validation
  - Entrust LibKmp Library Buffer Overflow
  - Hastymail Email 'Download' Arbitrary Code
  - Icecast Cross-Site Scripting
  - Mantis 't_core_dir' Variable
  - Mantis Cross-Site Scripting & HTML Injection
  - meindlSOFT Cute PHP Library (cphplib) Input Validation
  - **Mozilla Multiple Vulnerabilities (updated)**
  - Multiple Vendor NSS Buffer Overflow
  - Network Everywhere Router Remote Script Injection
  - Novell iChain Multiple Unspecified Remote Vulnerabilities
  - Opera Web Browser Resource Detection
  - PhotoADay Pad_selected Parameter Cross-Site Scripting

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

Risk is defined as follows:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature shoul instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
altSoft aGSM 2.35 c	A buffer overflow vulnerability exists in the server information parsing routines for Half-Life game servers due to a boundary error when receiving information, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	aGSM Half-Life Server Info Response Buffer Overflow	High	Secunia Adviso SA12334, Augu 24, 2004
birdchat.sourceforge.net Internet Chat Server 1.61	A remote Denial of Service vulnerability exists due to insufficient sanitization of user-supplied input. No workaround or patch available at time of publishing. An exploit script has been published.	Bird Chat Remote Denial of Service	Low	Securiteam, August 25, 200
Cisco Systems Access Control Server Solution Engine, Secure Access Control Server 3.2 (3), 3.2 (2), 3.2, Secure ACS for Windows Server 3.2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the web-based management interface (CSAdmin); a remote Denial of Service vulnerability exists when processing LEAP (Light Extensible Authentication Procotol) authentication requests when the device is configured as a LEAP RADIUS proxy; a vulnerability exists when handling NDS (Novell Directory Services) users, which could let a remote malicious user bypass authentication; and a vulnerability exists in the ACS administration web services, which could let a remote malicious user bypass authentication. Workaround and patches available at: http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml There is no exploit code required.	Secure Access Control Server Multiple Remote Vulnerabilities	Low/Medium (Medium if authentication can be bypassed)	Cisco Security Advisory, 61603 August 25, 200
EFS Software Inc. Easy File Sharing Web Server 1.2, 1.25	Several vulnerabilities exist: a vulnerability exists due to insufficient restrictions on the web server's virtual folders, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user submits several large HTTP requests. No workaround or patch available at time of publishing. There is no exploit code required.	Easy File Sharing Web Server Information Disclosure & Remote Denial of Service	Low/Medium (Medium if sensitive information can be obtained)	GulfTech Secur Research Advisory, Augus 24, 2004
gadu-gadu.pl Gadu-Gadu Instant Messenger 6.0	A vulnerability exists because a link can be created with a specially crafted filename, which could let a remote malicious user send a file with a spoofed file extension. No workaround or patch available at time of publishing. There is not exploit code required; however, a Proof of Concept exploit has been published.	Gadu-Gadu Spoofed File Extension	Medium	SecurityTracker Alert ID, 101103 August 24, 200
Ipswitch WhatsUp Gold 7.0 4, 7.0 3, 7.0, 8.0 3, 8.0 1, 8.0	A buffer overflow vulnerably exists in the '_maincfgret.cgi' script due to a failure to validate user-supplied string lengths, which could let a remote malicious user execute arbitrary code. Upgrades available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/WhatsUp/wug803HF1.exe We are not aware of any exploits for this vulnerability.	WhatsUp Gold Remote Buffer Overflow CVE Name: CAN-2004-0798	High	iDEFENSE Security Adviso August 25, 200
Keene Software Corporation Keene Digital Media Server 1.0.2	A Directory Traversal vulnerability exists when files are requested outside of the webroot of the application using hex encoded character sequences, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	Keene Digital Media Server Directory Traversal	Medium	Securiteam, August 30, 200
Massive Entertainment Ground Control II 1.0 .0.7	A remote Denial of Service vulnerability exists when a game client or server receives a packet larger than 512 bytes. No workaround or patch available at time of publishing. Proof of Concept exploit script has been published.	Ground Control II Remote Denial of Service	Low	Securiteam, August 30, 200
Merak Mail Server, Inc. Merak Mail Server 7.4.5	Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist due to insufficient validation of user-supplied input in a number of variables, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists because specially crafted HTML can be injected directly into a message or included in the subject field, which could let a remote malicious user execute arbitrary code; a vulnerability exists in 'adress.html' or 'calendar.html' when a remote malicious user submits specially crafted parameters which results in the disclosure of sensitive information; a vulnerability exists because a remote malicious user can download any file with a '.php' extension which results in the disclosure of sensitive information; and a vulnerability exists in 'calendar.html' because a remote malicious user can inject SQL commands. Upgrade available at: http://www.merakmailserver.com/Download/clickthrough.asp?file=merakhttpzip There is no exploit code required; however, Proofs of Concept exploits have been published.	Merak Mail Server Webmail Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Securiteam, August 19, 200
Microsoft Internet Explorer 5.0, 6.0, SP1	A vulnerability exists because an IFRAME that is accessible in the same domain may be used to change the URI to the location of a file or directory, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing.	Internet Explorer Resource Detection	Medium	Bugtraq, Augus 24, 2004

	Proof of Concept exploit has been published.			
Microsoft Internet Explorer 5.5, SP1&SP2. 6.0, SP1	A vulnerability exists due to insufficient validation of drag and drop events issued from the 'Internet' zone, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	Internet Explorer Drag & Drop File Installation	High	Secunia Adviso SA12321 Augus 19, 2004
Microsoft Internet Explorer 6.0 SP1	A cross security domain script vulnerability exists when a malicious MHTML file is submitted, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit script has been published.	Internet Explorer MHTML Content-Location Cross Security Domain Scripting	High	Bugtraq, Augus 19, 2004
Microsoft Outlook Express 6.0, SP1	A vulnerability exists in the 'bcc:' field due to an error when sending multipart messages, which could let a remote malicious user obtain sensitive information. Hotfix available at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;843555 There is no exploit code required.	Outlook Express BCC Field Information Disclosure	Medium	Secunia Adviso SA12376, Augu 25, 2004
Microsoft Small Business Server 2000, 2003, Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, 2000 Server Japanese Edition, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP 64-bit Edition Version 2003, SP1, XP Embedded. SP1, XP Embedded XP Professional, SP1&SP2l	A time spoofing vulnerability exists in the Network Time Protocol (NTP) implementation because the time on the domain controller can be altered, which could let a remote malicious user cause a Denial of Service and possibly other attacks. Microsoft has released a knowledge base article (884776) describing methods of mitigation. This article recommends that a hardware time source be used on the authoritative time server, instead of an unauthenticated network time source. We are not aware of any exploits for this vulnerability.	Microsoft NTP Time Synchronization Spoof	Low	SecurityFocus, August 19, 200
NakedSoft Gaucho 1.4 build 145	A buffer overflow vulnerability exists in the 'Content-Type:'"header due to insufficient validation, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://homepage1.nifty.com/nakedsoft/Gaucho/G-14B151.zip Proof of Concept exploit script has been published.	Gaucho POP3 Email Header Buffer Overflow	High	SIG^2 Vulnerab Research Advisory, Augus 23, 2004
Nihuo Software, Inc. Web Log Analyzer 1.6	A Cross-Site Scripting vulnerability exists in the 'user-agent' and referer' fields due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is not exploit code required; however, a Proof of Concept exploit has been published.	Web Log Analyzer Cross-Site Scripting	High	SecurityTracker 1011010, Augus 21, 2004
NullSoft Winamp 2.4, 2.5 e, 2.5 E, 2.6 4, 2.10, 2.24, 2.50, 2.60 (lite), 2.60 (full), 2.61 (full), 2.62 (standard), 2.64 (standard), 2.65, 2.70 (full), 2.70, 2.71-2.81, 2.91, 3.0, 3.1, 5.0 1- 5.04	A vulnerability exists due to insufficient restrictions on Winamp skin zip files (.wsz), which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.winamp.com/player/ This issue is known to be exploited in the wild and a Proof of Concept exploit has been published.	Winamp Skin File Remote Code Execution	High	Bugtraq, Augus 26, 2004
Pedestal Software Integrity Protection Driver 1.2, 1.3, 1.4	A Denial of Service vulnerability exists due to improperly validation of some pointer references in some of the application's kernel hooks. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Integrity Protection Driver Local Denial of Service	Low	Next Generatio Security Technologies Security Adviso NGSEC-2004-6 August 14, 200
People Can Fly Painkiller 1.3.1	A buffer overflow vulnerability exists due to insufficient boundary checking when processing a password supplied by a client during the connection establishment, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	Painkiller Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Securiteam, August 29, 200
RealVNC RealVNC 4.0	A remote Denial of Service vulnerability exists when a malicious user establishes a large amount of connections. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	RealVNC Server Remote Denial of Service	Low	SecurityTracker Alert ID: 10110 August 26, 200
Sysinternals Regmon 6.11	A Denial of Service vulnerability exists due to insufficient validation of some argument pointers. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Regmon Local Denial of Service	Low	Next Generatio Security Technologies Security Adviso NGSEC-2004-7 August 14, 200
Webroot Software, Inc Window Washer 5.5	A vulnerability exists in the 'AddBleach to Wash' function because the content of erased files is not properly overwritten, which could let a malicious user person modify system information. No workaround or patch available at time of publishing. There is no exploit code required.	Webroot Window Washer Erased Files	Medium	Secunia Adviso SA12380, Augu 26, 2004
Working Resources Inc. BadBlue 2.5	A remote Denial of Service vulnerability exists when processing multiple connections. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	BadBlue Webserver Denial of Service	Low	GulfTech Secur Research Advisory, Augus 18, 2004
Zone Labs ZoneAlarm 2.1-2.6, 3.0, 3.1, 3.7 .202, 4.0, 4.5 .538.001, ZoneAlarm for Windows 95 1.0, 2.2-2.6, ZoneAlarm for Windows 98 2.1-2.6, ZoneAlarm For Windows NT 4.0 2.1-4.0 2.6, ZoneAlarm for Windows XP 2.6, ZoneAlarm Plus 4.0, 4.5.538.001, ZoneAlarm Pro 2.4, 2.6, 3.0, 3.1, 4.0, 4.5.538.001, 4.5, 5.0.590.015	A vulnerability exists due to weak default permissions in the folder used to store log and configuration files, which could let a malicious user delete log entries in order to hide malicious activities. No workaround or patch available at time of publishing. There is not exploit code required.	ZoneAlarm/ZoneAlarm Pro Weak Default Permissions	Medium	Bugtraq, Augus 20, 2004

[back to top]

http://security.debian.org/pool/updates/main/r/ruby/

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Adobe Systems Adobe Acrobat Reader 5.05 and 5.06	An input validation and boundary error vulnerability exists in in the uudecoding feature of Adobe Acrobat Reader, which can be exploited by a malicious user to compromise a user's system. An input validation error injection of arbitrary shell commands. The boundary vulnerability can be exploited to cause a buffer overflow via a malicious PDF document with an overly long filename. Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into opening a malicious document. Update to version 5.09 for UNIX available at: http://www.adobe.com/products/acrobat/readstep2.html **Gentoo: http://security.gentoo.org/glsa/glsa-200408-14.xml** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-432.html** We are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader Shell Command Injection and Buffer Overflow Vulnerability CVE Names: CAN-2004-0630 CAN-2004-0631	High	Secunia, SA1228 August 13, 2004 iDEFENSE Advisories 08.12. **Gentoo Linux Security Adviso GLSA 200408-14 August 15, 2004** **RedHat Security Advisory, RHSA 2004:432-08, August 26,2 004**
Anton Raharja PlaySMS 0.6, 0.7	An input validation vulnerability exists in the 'valid()' function if the 'magic_quotes_gpc' setting if set to 'Off' due to insufficient verification, which could let a remote malicious user execute arbitrary SQL commands. Upgrades available at: http://prdownloads.sourceforge.net/playsms/playsms-0.7.1.tar.gz?download Proof of Concept exploit script has been published.	PlaySMS SQL Input Validation	High	Securiteam, Augu 18, 2004
Apple OS X Safari	A vulnerability exists in the 'Show in Finder' option, which could let a malicious user execute arbitrary code. Update available at: http://docs.info.apple.com/article.html?artnum=25785 We are not aware of any exploits for this vulnerability.	Mac OS X Safari 'Show in Finder' CVE Name: CAN-2004-0539	High	US-CERT Vulnerability Note VU#773190, Aug 24,2 004
Ben Yacoub Hatem MySQL Backup Pro 1.0.5-1.0.7	A vulnerability exists in the 'getbackup()' function, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://freshmeat.net/redir/phpmysqlbackupro/49350/url_zip/1 We are not aware of any exploits for this vulnerability.	MySQL Backup Pro Information Disclosure	Medium	SecurityFocus, August 20, 2004
Bharat Mediratta Gallery 1.4.4	A vulnerability exists in the 'set_time_limit' function due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://prdownloads.sourceforge.net/gallery/ Proof of Concept exploit has been published.	Gallery Input Validation	High	SecurityTracker A ID: 1010971, Aug 18, 2004
British National Corpus SARA	A remote buffer overflow vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	SARA Remote Buffer Overflow	High	Bugtraq, August 2 2004
Double Precision, Inc. Inter7 Courier-IMAP 1.6, 1.7, 2.0 .0, 2.1-2.1.2, 2.2 .0. 2.2.1	A format string vulnerability exists in the 'auth_debug()' function used for login debugging, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://prdownloads.sourceforge.net/courier/courier-imap-3.0.7.tar.bz2 Gentoo: http://security.gentoo.org/glsa/glsa-200408-19.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ We are not aware of any exploits for this vulnerability.	Courier-IMAP Remote Format String CVE Name: CAN-2004-0777	High	iDEFENSE Secu Advisory 08.18.0
EnderUNIX SDT Hafiye 1.0	A vulnerability exists due to insufficient filtering when a packet payload is displayed, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Hafiye Terminal Escape Sequence	High	SecurityFocus, August 23, 2004
fidogate.org FIDOGATE 4.4.5-4.4.7, 4.4.9	An input validation vulnerability exists in '/src/common/log.c' which could let a malicious user obtain elevated privileges. Upgrades available at: http://prdownloads.sourceforge.net/fidogate/fidogate-4.4.10.tar.gz?download There is no exploit code required.	FIDOGATE Input Validation	Medium	SecurityTracker A ID: 1011021, Aug 23, 2004
Gaim Gentoo	Multiple vulnerabilities were reported in Gaim in the processing of the MSN protocol. A remote user may be able to execute arbitrary code on the target system. Several remotely exploitable buffer overflows were reported in the MSN protocol parsing functions. Gentoo: http://security.gentoo.org/glsa/glsa-200408-12.xml SuSE: http://www.suse.de/de/security/2004_25_gaim.html **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425** **Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.1/patches/packages/gaim-0.82-i486-1.tgz** We are not aware of any exploits for this vulnerability.	Gaim Buffer Overflows in Processing MSN Protocol CVE Name: CAN-2004-0500	High	SecurityTracker, 1010872, August 2004 **Mandrakelinux Security Update Advisory, MDKS 2004:081, Augus 13, 2004** **Slackware Secu Advisory, SSA:2004-239-0 August 26, 2004**
GNU a2ps 4.13	A vulnerability exists in filenames due to insufficient validation of shell escape characters, which could let a malicious user execute arbitrary commands. FreeBSD: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain There is no exploit code required; however, a Proof of Concept exploit has been published.	GNU a2ps Command Injection	High	Securiteam, Augu 29, 2004
Hitachi	Multiple vulnerabilities exist: a vulnerability exists in the login authentication procedure, which could	Hitachi Job Management	Low/Medium	HS04-004-01 &

Job Management Partner-1 6 & 7	when a malicious user submits a specially crafted reset packet. Upgrades available at:/http://www.hitachi-support.com/security_e/ We are not aware of any exploits for this vulnerability.	Flaw & Remote Denial of Service	(Medium if unauthorized access can be obtained)	August 23, 2004
imwheel.sourceforge.net IMWheel 1.0 pre11	A vulnerability exists due to a race condition and insecure creation of a temporary file ('/tmp/imwheel.pid') used for managing running imwheel processes, which could let a malicious user cause a Denial of Service or obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	IMWheel Insure File Creation	Low/Medium (Medium is elevated privileges can be obtained)	Computer Acade Underground Security Advisory CAU-2004-0002, August 26, 2004
InfoTecna s.r.l. sredird 1.0, 1.1.6-1.1.8, 2.0, 2.1, 2.2, 2.2.1; Peter Åstrand SERCD 2.3 .0	Two vulnerabilities exist: a format string vulnerability exists in the 'LogMsg()' function due to insufficient sanitization, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'HandleCPCCommand()' function due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www.lysator.liu.se/~astrand/projects/sercd/sercd-2.3.1.tar.gz We are not aware of any exploits for this vulnerability.	SERCD, SREDIRD Format String & Buffer Overflow	High	SecurityTracker A ID: 1011038, Aug 24, 2004
INL Ulog-php 0.8, 0.8.1	An input validation vulnerability exists in 'port.php' due to insufficient validation of the 'proto' parameter, which could let a remote malicious user execute arbitrary SQL commands. Upgrades available at: http://www.inl.fr/download/ulog-php-0.8.2.tar.gz There is no exploit code required.	Ulog-php Input Validation	High	SecurityFocus, August 23, 2004
Inter7 vpopmail (vchkpw) 3.4.1-3.4.11, 4.5, 4.6, 4.7, 4.8, 4.9, 4.9.10, 4.10, 5.2.1, 5.2.2, 5.3.20-5.3.30, 5.4-5.4.2	Multiple buffer overflow and format string vulnerabilities exist in the 'vsybase.c' file, which could let a malicious user cause a Denial of Service, obtain unauthorized access, or execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/vpopmail/vpopmail-5.4.6.tar.gz?download We are not aware of any exploits for this vulnerability.	Inter7 Vpopmail Vsybase.c Multiple Vulnerabilities	Low/ Medium/High Low if a DoS; Medium if unauthorized access can be obtained; and High if arbitrary code can be executed.	Bugtraq, August 2004
Inter7 vpopmail (vchkpw) 3.4.1-3.4.11, 4.5-4.10, 5.2.1, 5.2.2, 5.3.20-5.3.30, 5.4-5.4.5	An SQL injection vulnerability exists due to insufficient sanitization of user-supplied input data before using it in an SQL query, which could let a remote malicious user insert additional SQL commands into data passed into POP/IMAP login, SMTP AUTH, or a QmailAdmin login. *Note: Vpopmail is only vulnerable if SQL servers are utilized by the application. Sites using the 'cdb' backend for data storage are not affected.* Upgrades available at: http://prdownloads.sourceforge.net/vpopmail/vpopmail-5.4.6.tar.gz?download There is no exploit code required.	Vpopmail SQL Injection	Medium	SecurityFocus, August 20, 2004
John Bradley XV 3.10 a	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'xvbmp.c' source file, which could let a remote malicious user execute arbitrary code; multiple heap overflow vulnerabilities exist in the 'xviris.c' source file due to integer handling problems, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists in the 'xvpcx.c' source file due to integer handling problems, which could let a remote malicious user execute arbitrary code; and a heap overflow vulnerability exists in the 'xvpm.c' source file due to integer handling problems, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Exploit script has been published.	XV Multiple Buffer Overflow and Integer Handling	High	Bugtraq, August 2004
Linux Fedora RedHat SuSE Linux kernel 2.4 through 2.4.26, 2.6 through 2.6.7	A vulnerability exists in the Linux kernel in the processing of 64-bit file offset pointers thus allowing a local malicious user to view kernel memory. The kernel's file handling API does not properly convert 64-bit file offsets to 32-bit file offsets. In addition, the kernel provides insecure access to the file offset member variable. As a result, a local user can gain read access to large portions of kernel memory. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/ SuSE: http://www.suse.de/de/security/2004_24_kernel.html **Gentoo:http://security.gentoo.org/glsa/glsa-200408-24.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/** **Trustix: ftp://ftp.trustix.org/pub/trustix/updates/** A Proof of Concept exploit script has been published.	Linux Kernel 64-bit to 32-bit File Offset Conversion Errors Disclose Kernel Memory to Local Users CVE Name: CAN-2004-0415	High	ISEC Security Research, Augus 2004 **SGI Security Advisory, 20040804-01-U, August 26, 2004** **Gentoo Linux Security Adviso GLSA 200408-24 August 25, 2004** **Mandrakelinux Security Update Advisory, Augus 26, 2004** **Trustix Secure Linux Security Advisory, TSLSA 2004-0041, Augu 9, 2004**
Marc Lehmann RXVT-Unicode 3.4, 3.5	A vulnerability exist due to a failure to properly close file descriptors when spawning new child terminal windows, which could let a malicious user obtain sensitive information. Update available at: http://dist.schmorp.de/rxvt-unicode/rxvt-unicode-3.6.tar.bz2 There is no exploit code required.	RXVT-Unicode Open File Descriptor Leakage	Medium	Secunia Advisory SA1229, August 2004
Multiple Vendors FileZilla Server 0.7, 0.7.1; OpenBSD -current, 3.5; OpenPKG Current, 2.0, 2.1; zlib 1.2.1	A remote Denial of Service vulnerability during the decompression process exists due to a failure to handle malformed input. . Gentoo: http://security.gentoo.org/glsa/glsa-200408-26.xml FileZilla: http://sourceforge.net/project/showfiles.php?group_id=21558 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz.patch OpenPKG: ftp ftp.openpkg.org Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ We are not aware of any exploits for this vulnerability.	Zlib Compression Library Remote Denial of Service CVE Name: CAN-2004-0797	Low	SecurityFocus, August 25, 2004
Multiple Vendors	A vulnerability exists in 'LD_DEBUG' on set user id (setuid) binaries, which could let a malicious	GLibC LD_DEBUG	Medium	Gentoo Linux

Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, rc1-rc3; GNU glibc 2.0-2.0.6, 2.1, 2.1.1-6, 2.1.1, 2.1.2, 2.1.2-10, 2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3-2.3.4	Gentoo: http://security.gentoo.org/glsa/glsa-200408-16.xml We are not aware of any exploits for this vulnerability.			GLSA 200408-16 August 16, 2004
Multiple Vendors Gentoo Linux 1.4; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1, Desktop 3.0, t Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, 2.1 IA64, 2.1, AS 3, AS 2.1 IA64, AS 2.1' Trolltech Qt 3.0, 3.0.5, 3.1, 3.1.1, 3.1.2, 3.2.1, 3.2.3, 3.3 .0, 3.3.1, 3.3.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'read_dib()' function when handling 8-bit RLE encoded BMP files, which could let a malicious user execute arbitrary code; and buffer overflow vulnerabilities exist in the in the XPM, GIF, and JPEG image file handlers, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/qt-copy/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/qt-3.1.2-i486-4.tgz SuSE: ftp://ftp.suse.com/pub/suse/i386/update Trolltech Upgrade: http://www.trolltech.com/download/index.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Proof of Concept exploit has been published.	Qt Image File Buffer Overflows CVE Names: CAN-2004-0691, CAN-2004-0692, CAN-2004-0693	High	Secunia Advisory SA12325, August 10, 2004
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.1.3, 3.2, 3.0- 3.0.3, 3.0.5b, 3.0.5, 3.1-3.1.3, 3.1.5, 3.2.1, 3.2.3; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64	A vulnerability exists while validating cookie domains, which could let a remote malicious user hijack a target user's session. KDE: ftp://ftp.kde.org/pub/kde/security_patches Gentoo: http://security.gentoo.org/glsa/glsa-200408-23.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit code required.	KDE Konqueror Cookie Domain Validation CVE Name: CAN-2004-0746	Medium	KDE Security Advisory, August 2004
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3; MandrakeSoft Linux Mandrake 9.2 amd64, 9.2, 10.0 AMD64, 10.0	A vulnerability exists due to insufficient validation of ownership of temporary directories, which could let a malicious user cause a Denial of Service, overwrite arbitrary files, or obtain elevated privileges. KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.0.5b-kdelibs-kstanderddirs.patch Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit code required.	KDE Insecure Temporary Directory Symlink CVE Name: CAN-2004-0689	Low/Medium (Low if a DoS)	KDE Security Advisory,August 2004
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.2-3.2.3; MandrakeSoft Linux Mandrake 9.2 amd64, 9.2, 10.0 AMD64, 10.0	A vulnerability exists in DCOPServer due to insecure file creation, which could let a malicious user obtain elevated privileges or overwrite arbitrary files. KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-dcopserver.patch Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit code required.	KDE DCOPServer Insecure Temporary File Creation CVE Name: CAN-2004-0690	Medium	KDE Security Advisory,August 2004
Multiple Vendors KDE 3.2.3 and prior	A frame injection vulnerability exists in the Konqueror web browser that allows websites to load web pages into a frame of any other frame-based web page that the user may have open. A malicious website could abuse Konqueror to insert its own frames into the page of an otherwise trusted website. As a result the user may unknowingly send confidential information intended for the trusted website to the malicious website. Source code patches have been made available which fix these vulnerabilities. Refer to advisory: http://www.kde.org/info/security/advisory-20040811-3.txt **Mandrake: http://www.mandrakesecure.net/en/ftp.php** A Proof of Concept exploit has been published.	Konqueror Frame Injection Vulnerability CVE Name: CAN-2004-0721	Low	KDE Security Advisory 200408 3, August 11, 200 **Mandrakelinux Security Update Advisory, MDKS 2004:086, Augus 21, 2004**
Multiple Vendors Linux kernel 2.4 .0-test1-test9, Linux kernel 2.4-2.4.26, 2.6 -test1-test9, 2.6-2.6.7	A race condition vulnerability exists when a process is spawning, which could let a malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200408-24.xml We are not aware of any exploits for this vulnerability.	Linux Kernel Race Condition	Medium	Gentoo Linux Security Advisory GLSA 200408-24 August 25, 2004
Multiple Vendors Luke Mewburn lukemftp 1.5, TNFTPD 20031217; NetBSD Current, 1.3-1.3.3, 1.4 x86, 1.4, SPARC, arm32, Alpha, 1.4.1 x86, 1.4.1, SPARC, sh3, arm32, Alpha, 1.4.2 x86, 1,4.2, SPARC, arm32, Alpha, 1.4.3, 1.5 x86, 1.5, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6-1.6.2, 2.0	Several vulnerabilities exist in the out-of-band signal handling code due to race condition errors, which could let a remote malicious user obtain superuser privileges. Luke Mewburn Upgrade: ftp://ftp.netbsd.org/pub/NetBSD/misc/tnftp/tnftpd-20040810.tar.gz We are not aware of any exploits for this vulnerability.	TNFTPD Multiple Signal Handler Remote Privilege Escalation	High	NetBSD Security Advisory 2004-00 August 17, 2004
Multiple Vendors Mozilla Browser 1.7.2, Mozilla Firefox 0.9.3; Netscape Navigator 7.1, 7.2	A vulnerability exists when the browser is configure to employ the 'Tabbed Browsing' functionality, which could let a remote malicious user conduct phishing attacks. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	Mozilla/Netscape/Firefox Browsers Content Spoofing	Medium	Bugtraq, August 2004
musicdaemon.sourceforge.net Music daemon 0.1-0.3	A vulnerability exists due to insufficient authentication of user-supplied commands, which could let a remote malicious user obtain sensitive information information or cause a Denial of Service. No workaround or patch available at time of publishing. An exploit script has been published.	Music Daemon Information Disclosure	Low/Medium (Medium if sensitive information can be obtained)	Securiteam, Augu 26, 2004
MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21 .x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0.0-4.0.15, 4.0.18, 4.0.20, 4.1 .0-alpha,	A buffer overflow vulnerability exists in the 'mysql_real_connect' function due to insufficient boundary checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. *Note: Computers using glibc on Linux and BSD platforms may not be vulnerable to this issue.* No workaround or patch available at time of publishing.	MySQL Mysql_real_connect Function Remote Buffer Overflow	High/Low (Low if a DoS)	Secunia Advisory SA12305, August 20, 2004

0, 5.0 .0-alpha, 5.0 .0-0				
MySQL AB MySQL 3.23.49, 4.0.20	A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/ There is no exploit code required.	MySQL 'Mysqlhotcopy' Script Elevated Privileges CVE Name: CAN-2004-0457	Medium	Debian Security Advisory, DSA 54 1, August 18, 200
OpenBSD OpenBSD 3.2-3.5	A Denial of Service vulnerability exists in the implementation of bridging in OpenBSD due to insufficient validation of ICMP packets. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ There is no exploit code required.	OpenBSD Bridged Network ICMP Denial of Service	Low	Bugtraq, August 2004
OpenBSD OpenBSD –current, 3.3, 3.4	Multiple remote Denial of Service vulnerabilities exist when processing certain malformed payloads. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ We are not aware of any exploits for this vulnerability.	OpenBSD isakmpd Multiple Unspecified Remote Denial of Service CVE Names: CAN-2004-0218, CAN-2004-0219, CAN-2004-0220, CAN-2004-0221, CAN-2004-0222	Low	SecurityFocus, March 23, 2004 **US-CERT Vulnerability No VU#223273, VU#349113, VU#524497, VU#785945, VU#996177, Aug 27, 2004**
PHP Code Snippet Library PHP Code Snippet Library 0.8	Multiple Cross-Site Scripting vulnerabilities exist in 'index.php' due to insufficient sanitization of the 'cat_select' and 'show' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP Code Snippet Library Multiple Cross-Site Scripting	High	Secunia Advisory SA12370, August 25, 2004
Raxnet Cacti 0.5, 0.6-0.6.8, 0.8-0.8.5; Gentoo Linux 1.4	A vulnerability exists in the 'auth_login.php' script due to insufficient validation of user-supplied input in the username or password fields, which could let a remote malicious user bypass the authentication interface. The vendor has issued a fix, available via CVS. Gentoo: http://security.gentoo.org/glsa/glsa-200408-21.xml Proofs of Concept exploits have been published.	RaXnet Cacti Auth_Login.PHP Authentication Bypass	Medium	SecurityTracker A ID: 1010961, Aug 17, 2004
RedHat GNOME VFS Red Hat Enterprise Linux AS (Advanced Server) version 2.1 - i386, ia64; Red Hat Linux Advanced Workstation 2.1 - ia64; Red Hat Enterprise Linux ES version 2.1 - i386; Red Hat Enterprise Linux WS version 2.1 - i386; Red Hat Enterprise Linux AS version 3 - i386, ia64, ppc, s390, s390x, x86_64 Red Hat Desktop version 3 - i386, x86_64; Red Hat Enterprise Linux ES version 3 - i386, ia64, x86_64; Red Hat Enterprise Linux WS version 3 - i386, ia64, x86_64	Multiple vulnerabilities exist in several of the GNOME VFS exists backend scripts, which could let a malicious user influence a user to open a specially-crafted URI using gnome-vfs could perform actions as that user. Users of Red Hat Enterprise Linux should upgrade to these updated packages, which remove these unused scripts. Before applying this update, make sure that all previously-released errata relevant to your system have been applied. Use Red Hat Network to download and update your packages. To launch the Red Hat Update Agent, use the following command: up2date For information on how to install packages manually, refer to the following Web page for the System Administration or Customization guide specific to your system: http://www.redhat.com/docs/manuals/enterprise/ **SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/** We are not aware of any exploits for this vulnerability.	GNOME VFS updates address exists vulnerability CVE Name: CAN-2004-0494	High	Red Hat Security Advisory ID: RHS 2004:373-01, Aug 4, 2004 **SGI Security Advisory, 20040802-01-U, August 14, 2004**
Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75	Multiple vulnerabilities exist which could let a remote malicious user execute arbitrary code or cause a Denial of Service: a vulnerability exists during the installation of a smiley theme; a heap overflow vulnerability exists when processing data from a groupware server; a buffer overflow vulnerability exists in the URI parsing utility; a buffer overflow vulnerability exists when performing a DNS query to obtain a hostname when signing on to zephyr; a buffer overflow vulnerability exists when processing Rich Text Format (RTF) messages; and a buffer overflow vulnerability exists in the 'content-length' header when an excessive value is submitted. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo:http://security.gentoo.org/glsa/glsa-200408-27.xml Rob Flynn: http://sourceforge.net/project/showfiles.php?group_id=235&package_id=253&release_id=263425 Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.0/patches/packages/gaim-0.82-i486-1.tgz We are not aware of any exploits for this vulnerability.	Gaim Multiple Vulnerabilities CVE Names: CAN-2004-0784, CAN-2004-0754, CAN-2004-0785	Low/High (High if arbitrary code can be executed)	SecurityFocus, August 26, 2004
rsync 2.6.2 and prior Debian SuSE Trustix	A vulnerability exists in rsync when running in daemon mode with chroot disabled. A remote user may be able read or write files on the target system that are located outside of the module's path. A remote user can supply a specially crafted path to cause the path cleaning function to generate an absolute filename instead of a relative one. The flaw resides in the sanitize_path() function. Updates and patches are available at: http://rsync.samba.org/ SuSE: http://www.suse.de/de/security/2004_26_rsync.html Debian: http://www.debian.org/security/2004/dsa-538 Trustix: http://www.trustix.net/errata/2004/0042/ **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **Gentoo: http://security.gentoo.org/glsa/glsa-200408-17.xml** **Netwosix: http://www.netwosix.org/adv17.html** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/rsync-2.6.0-2.0.2.src.rpm**	Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or Write Arbitrary Files	High	SecurityTracker 1010940, August 2004 rsync August 200 Security Advisory **OpenPKG Secur Advisory, OpenPKG-SA-2004.037, Augus 15, 2004** **Tinysofa Securit Advisory, TSSA-2004-020-ES, August 16, 2004** **Gentoo Linux Security Advisor GLSA 200408-17 August 17, 2004** **Netwosix Linux**

	2.0/i386/tinysofa/rpms.updates/rsync-2.6.2-2ts.i386.rpm **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/** We are not aware of any exploits for this vulnerability.			**LNSA-#2004-001 August 17, 2004** **Mandrakelinux Security Update Advisory, MDKS 2004:083, Augus 17, 2004** **Fedora Update Notification, FEDORA-2004-2 August 19, 2004** **Turbolinux Security Adviso TLSA-2004-20, August 31, 2004**
Samba Samba 2.2.11, 3.0.6	A remote Denial of Service vulnerability exists due to the way print change notify requests are processed. Trustix: http://http.trustix.org/pub/trustix/updates/ We are not aware of any exploits for this vulnerability.	Samba Remote Print Change Notify Remote Denial of Service	Low	Trustix Secure Li Security Advisory TSL-2004-0043, August 26, 2004
sox.sourceforge.net Fedora Mandrakesoft Gentoo Conectiva RedHat SoX 12.17.4, 12.17.3, and 12.17.2	Multiple vulnerabilities exist that could allow a remote malicious user to execute arbitrary code This is due to boundary errors within the "st_wavstartread()" function when processing ".WAV" file headers and can be exploited to cause stack-based buffer overflows. Successful exploitation requires that a user is tricked into playing a malicious ".WAV" file with a large value in a length field. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:076 Gentoo: http://security.gentoo.org/glsa/glsa-200407-23.xml Conectiva: ftp://atualizacoes.conectiva.com.br RedHat: http://rhn.redhat.com/errata/RHSA-2004-409.html **Slackware: ftp://ftp.slackware.com/pub/slackware/** **SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/** Exploit script has been published.	**SoX ".WAV" File Processing Buffer Overflow Vulnerabilities** **CVE Name: CAN-2004-0557**	High	Secunia, SA1217 12176, 12180, Ju 29, 2004 SecurityTracker Alerts 1010800 a 1010801, July 28 2004 Mandrakesoft Security Advisory MDKSA-2004:07 July 28, 2004 PacketStorm, August 5, 2004 **Slackware Secu Advisory, SSA:2004-223-0 august 10, 2004** **SGI Security Advisory, 20040802-01-U, August 14, 2004**
SpamAssassin.org SpamAssassin prior to 2.64	A Denial of Service vulnerability exists in SpamAssassin. A a remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service. Update to version (2.64), available at: http://old.spamassassin.org/released/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** We are not aware of any exploits for this vulnerability.	SpamAssassin Remote Denial of Service	Low	SecurityTracker: 1010903, August 2004 **Mandrake Secur Advisory, MDKS 2004:084, Augus 19, 2004**
Sun Microsystems, Inc. DtMai, Solaris 8.0 _x86, 8.0, 9.0 _x86, 9.0	A buffer overflow vulnerability exists in the dtmailer when processing command line arguments, which could let a malicious user execute arbitrary code. Patches available at: http://sunsolve.sun.com/pub-cgi/ We are not aware of any exploits for this vulnerability.	Sun CDE Mailer Buffer Overflow CVE Name: CAN-2004-0800	High	Sun(sm) Alert Notification, 5762 August 23, 2004 US-CERT Vulnerability Note VU#928598, Aug 25, 2004
Sun Mircosystems, Inc. Solaris 7.0 _x86, 7.0, 8.0 _x86, 8.0, 9.0 _x86, 9.0	A buffer overflow vulnerability exists in 'LOGNAME' environment variables in CDE libDTHelp due to insufficient a lack of bounds checking, which could let a malicious user execute arbitrary code. Patches available at: http://sunsolve.sun.com/pub-cgi/ We are not aware of any exploits for this vulnerability.	CDE LibDTHelp LOGNAME Environment Variable Buffer Overflow	High	iDEFENSE Secu Advisory, August 2004
suPHP suPHP 0.3, 0.3.1, 0.5-0.5.2	A vulnerability exists due to insufficient validation during access control checks prior to executing PHP in a target file, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	SUPHP Elevated Privileges	Medium	Bugtraq, August 2004
SWsoft Plesk Reloaded 7.1	A Cross-Site Scripting vulnerability exists in 'login_up.php3' due to insufficient sanitization of the 'login_name' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Plesk 'Login_name' Parameter Cross-Site Scripting	High	Secunia Advisory SA12368, August 25, 2004
Sympa Sympa 3.x, 2.x, 4.0 .x, 4.1, 4.1.1	A vulnerability exists in 'wwsympa/wwsympa.fcgi' when creating new mailing lists, which could let a malicious user bypass authentication. Upgrades available at: http://www.sympa.org/distribution/sympa-4.1.2.tar.gz There is no exploit code required.	Sympa List Creation Authentication Bypass	Medium	Secunia Advisory SA12286, August 13, 2004
Sympa Sympa 4.0 .x, 4.1-4.1.2	A Cross-Site Scripting vulnerability exists in the 'description' field due to insufficient sanitization of user-supplied input data, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Sympa Cross-Site Scripting	High	Securiteam, Augu 22, 2004
web-app.org WebAPP 0.9.9	A Directory Traversal vulnerability exists in the 'index.cgi' script due to insufficient sanitization, which could let a remote malicious user obtain sensitive information.	WebAPP Directory Traversal	Medium	SecurityFocus, August 24, 2004

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
xine-Project xine 0.99.2	A buffer overflow vulnerability exists in xine in the processing of 'vcd://' protocol identifiers. A remote malicious user can execute arbitrary code on the target system. A remote malicious user can trigger a stack overflow in xine-lib by embedding a specially crafted source identifier within a playlist file, for example. When the target user plays the file, arbitrary code can be executed with the privileges of the target user. A patch is available via CVS at: http://sourceforge.net/mail archive/forum.php?thread_id=5143955&forum_id=11923 **Gentoo: http://security.gentoo.org/glsa/glsa-200408-18.xml** **A Proof of Concept exploit script has been published.**	xine Buffer Overflow in Processing 'vcd' Identifiers Lets Remote Users Execute Arbitrary Code	High	SecurityTracker: 1010895, August 2004 Open security advisory #6, Augu 8, 2004 **Gentoo Linux Security Adviso GLSA 200408-18 August 17, 2004**
Yukihiro Matsumoto Ruby 1.6, 1.8	A vulnerability exists in the CGI session management component due to the way temporary files are processed,which could let a malicious user obtain elevated privileges. Upgrades available at: http://security.debian.org/pool/updates/main/r/ruby/ We are not aware of any exploits for this vulnerability.	Ruby CGI Session Management Unsafe Temporary File CVE Name: CAN-2004-0755	Medium	Debian Security Advisory, DSA 53 1, August 16, 200

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
AWStats AWStats 5.0-5.9, 6.0-6.2	An input validation vulnerability exists in the 'awstats.pl' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. Proof of Concept exploit has been published.	AWStats 'awstats.pl' Input Validation	High	SecurityFocus August 19, 20
Axis Communications Firmware Version 2.40; Axis 2100/2110/2120/2420/2130, Network Camera, 2400/2401 Video Server	Multiple vulnerabilities exist: an input validation vulnerability exists in the '/axis-cgi/io/virtualinput.cgi' script, which could let a remote malicious user execute arbitrary commands; and a Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Axis Network Camera And Video Server Multiple Vulnerabilities	Medium/High (High if arbitrary commands can be executed)	Bugtraq, Augu 22, 2004
Axis Communications StorPoint CD	A vulnerability exists because a hard-coded administrative backdoor exists, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	StorPoint CD Administrative Backdoor	High	Bugtraq, Augu 22, 2004
Cisco Systems IOS 12.0S, 12.2, 12.3	A remote Denial of Service vulnerability exists when a malicious user continuously transmits malformed Open Shortest Path First (OSPF) packets. Updates available at: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml We are not aware of any exploits for this vulnerability.	IOS OSPF Remote Denial of Service	Low	Cisco Security Advisory, 613 August 21, 20 US-CERT Vulnerability N VU#989406
Cisco Systems IOS R12.x, 12.x	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted TCP connection to a telnet or reverse telnet port. Potential workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml We are not aware of any exploits for this vulnerability.	Cisco IOS Telnet Service Remote Denial of Service	Low	Cisco Security Advisory, cisc sa-20040827, August 27, 20 US-CERT Vulnerability N VU#384230
Dynix WebPac	Input validation vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	WebPAC Input Validation	High	Bugtraq, Augu 24, 2004
eGroupWare.org GroupWare 1.0, 1.0.3	Multiple Cross-Site Scripting vulnerabilities exist in the 'addressbook' and 'calendar' modules and HTML injections vulnerabilities exist in the 'Messenger' and 'Ticket' modules, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	EGroupWare Multiple Input Validation	High	Bugtraq, Augu 22, 2004
Entrust LibKMP ISAKMP Library	A buffer overflow vulnerability exists in the main SA payloads due to insufficient sanity checking, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Symantec: ftp://ftp.symantec.com/public/updates/ We are not aware of any exploits for this vulnerability.	Entrust LibKmp Library Buffer Overflow CVE Name: CAN-2004-0369	Low/High (High if arbitrary code can be executed)	Internet Secu Systems Protection Advisory, Aug 26, 2004
hastymail.sourceforge.net Hastymail 1.0.1, 1.1	A vulnerability exists when the 'download' link is invoked due to a failure to return the proper heading, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=66202&package_id=127017&release_id=262778 http://sourceforge.net/project/showfiles.php?group_id=66202&package_id=127016&release_id=262787 There is no exploit code required.	Hastymail Email 'Download' Arbitrary Code	High	Secunia Advisory, SA12358, Aug 24, 2004
Icecast.org Icecast 1.3 .10, 1.3 .0, 1.3.5 -1, 1.3.5, 1.3.7 -1, 1.3.7, 1.3.8 1.3.9 -2, 1.3.9 -1, 1.3.9, 1.3.10 -1, 1.3.11, 1.3.12	An Cross-Site Scripting vulnerability exists in 'src/http.c' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Debian: http://security.debian.org/pool/updates/main/i/icecast-server/ There is no exploit code required.	Icecast Cross-Site Scripting CVE Name: CAN-2004-0781	High	Debian Securi Advisory, DSA 541-1, August 24, 2004
Mantis Mantis 0.19 .0a	A vulnerability exists if the 'REGISTER_GLOBAL' because a remote malicious user can specify the 't_core_dir' variable to cause arbitrary code to be executed.	Mantis 't_core_dir' Variable	High	SecurityTrack Alert ID: 1011015, Aug

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
Mantis Mantis Mantis 0.9, 0.9.1, 0.10-0.10.2, 0.11, 0.11.1, 0.12, 0.13, 0.13.1, 0.14- 0.14.8, 0.15-0-0.15.12, 0.16.0, 0.16.1, 0.17.0 -0.17.5, 0.18a1, 0.180rc1, 0.18 0a4, 0.18 0a3, 0.18 0a2, 0.18, 0.19 .0a	Two vulnerabilities exist: a vulnerability exists in 'login_page.php' in the 'return' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists in 'signup.php' in the 'email' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary script code. Update available at: http://mantisbt.sourceforge.net/ There is no exploit code required; however, a Proof of Concept exploit has been published.	Mantis Cross-Site Scripting & HTML Injection	High	Secunia Advisory, SA12338, Aug 23, 2004
meindlSOFT Cute PHP Library (cphplib) 0.42-0.46	An Input validation vulnerability exist in the Cute PHP Library (cphplib) due to insufficient validation of certain parameters, which could let a remote malicious user executed arbitrary HTML code. Upgrade available at: http://www.meindlsoft.com/cphplib_download.php We are not aware of any exploits for this vulnerability.	Cute PHP Library (cphplib) Input Validation	High	SecurityFocus August 27, 20
Mozilla Organization Mandrakesoft Slackware Mozilla 1.7 and prior; Firefox 0.9 and prior; Thunderbird 0.7 and prior	Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads. Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082 **RedHat: http://rhn.redhat.com/errata/RHSA-2004-421.html** **SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/** We are not aware of any exploits for this vulnerability.	Mozilla Multiple Vulnerabilities CVE Name: CAN-2004-0757 CAN-2004-0759 CAN-2004-0761 CAN-2004-0765	High	Secunia, SA10856, Aug 4, 2004 **US-CERT Vulnerability Note VU#561** **RedHat Secu Advisory, RHSA-2004:4 17, August 4, 2004** **SGI Security Advisory, 20040802-01- August 14, 2**
Multiple Vendors HP HP-UX B.11.23, 11.11, 11.00; Mozilla Network Security Services (NSS) 3.2, 3.2.1, 3.3-3.3.2, 3.4-3.4.2, 3.5, 3.6, 3.6.1, 3.7-3.7.3, 3.7.5, 3.7.7, 3.8, 3.9; Netscape Certificate Server 1.0 P1, 4.2, Directory Server 1.3, P1&P5, 3.12, 4.1, 4.11-.4.13, Enterprise Server 2.0 a, 2.0, 2.0.1 C, 3.0 L, 3.0, 3.0.1 B, 3.0.1, 3.1, 3.2, 3.5, 3.6, SP1-SP3, 3.51, 4.0, 4.1, SP3-SP8, Enterprise Server for NetWare 4/5 3.0.7 a, 4/5 4.1.1, 4/5 5.0, Enterprise Server for Solaris 3.5, 3.6, Netscape Personalization Engine; Sun ONE Application Server 6.0, SP1-SP4, 6.5, SP1 MU1&MU2, 6.5 SP1, 6.5 MU1-MU3, 7.0 UR2 Upgrade Standard, 7.0 UR2 Upgrade Platform, Standard Edition, Platform Edition, 7.0 UR1 Standard Edition, Platform Edition, 7.0 Standard Edition, Platform Edition, Certificate Server 4.1, Directory Server 4.16, SP1, 5.0, SP1&SP2, 5.1 x86 SP3 x86, 5.1, SP1-SP3, 5.2, Web Server 4.1, SP1-SP14, 6.0, SP1-SP7, 6.1	A buffer overflow vulnerability exists in the Netscape Network Security Services (NSS) library suite due to insufficient boundary checks, which could let a remote malicious user which may result in remote execute arbitrary code. Mozilla:/ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_9_2_RTM/ We are not aware of any exploits for this vulnerability.	NSS Buffer Overflow	High	Internet Secu Systems Advisory, Aug 23, 2004
Network Everywhere NR041 1.2 Release 03	A vulnerability exists in the DHCP daemon due to insufficient sanitization of user-supplied input that is passed with the 'DHCP HOSTNAME' option, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Network Everywhere Router Remote Script Injection	High	Secunia Advisory, SA12393, Aug 27, 2004
Novell iChain Server 2.3	Multiple vulnerabilities exist: a vulnerability exists due to Insufficient validation of overly long UTF-8 encodings, which could let a remote malicious user bypass access control rules; a vulnerability exists due to insufficient sanitization of user-supplied input passed to the web server, which could let a remote malicious user execute arbitrary HTML and script code; a remote Denial of Service vulnerability exists when a remote malicious user submits a specially crafted URL; a vulnerability exists in the 'VIA' header, which could let a remote malicious user obtain sensitive information; and a vulnerability exists due to the insecure transmission of password and username credentials, which could let a remote malicious user obtain sensitive information. Patch available at : http://support.novell.com/servlet/filedownload/sec/ftf/b1ic23sp1.exe There is no exploit code required.	iChain Multiple Unspecified Remote Vulnerabilities	Low/Medium/High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Technical Information Document, TID2969621, August 24, 20
Opera Software Opera Web Browser 7.52, 7.53	A vulnerability exists in IFRAME, which could let a malicious user obtain sensitive information. Upgrades available at: http://www.opera.com/download/ Proof of Concept exploit has been published.	Opera Web Browser Resource Detection	Medium	GreyMagic Security Advis GM#009-OP, August 17, 20
PhotoADay.net PhotoADay	A Cross-Site Scripting vulnerability exists in the 'PhotoADay' PHP-Nuke module due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PhotoADay Pad_selected Parameter Cross-Site Scripting	High	SecurityTrack Alert ID, 1011027, Aug 23, 2004
PScript PForum 1.24, 1.25	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of the 'IRC Server' and 'AIM ID' fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.pscript.de/link/onelink.php?showid=6 There is no exploit code required; however, a Proof of Concept exploit has been published.	PScript PForum Cross-Site Scripting	High	Bugtraq, Augu 14, 2004 US-CERT Vulnerability N VU#674542, August 18,20(
pvpgn.org PvPGN 1.6 .0-1.6.3	A vulnerability exists in the 'passhash' attribute, which could let a remote malicious user obtain authentication information. Upgrades available at: http://prdownloads.sourceforge.net/pvpgn/pvpgn-1.6.4.tar.gz?download We are not aware of any exploits for this vulnerability.	PvPGN Information Disclosure	Medium	PvPGN Secur Advisory, PSA 20040823, August 23, 20
TikiWiki Project TikiWiki 1.8-1.8.2	Two vulnerabilities exist: a vulnerability exists because individual wiki page permissions can be bypassed, which could let a remote malicious user obtain unauthorized access; and a vulnerability exists in 'smarty_tiki' which could let a remote malicious user obtain sensitive information	TikiWiki Unauthorized Access &	Medium	SecurityTrack Alert ID: 1010962, Aug

	Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=64258&package_id=112133&release_id=257332 There is no exploit code required.	Disclosure		
Top Layer Networks TopLayer Attack Mitigator 5500 3.11 .008	A remote Denial of Service vulnerability exists when a malicious user submits a high volume of HTTP traffic. Update available at: http://www.toplayer.com/content/support/tech_assist/index.jsp There is no exploit code required.	Top Layer Attack Mitigator IPS 5500 Remote Denial of Service	Low	IRM Security Advisory No. 010, August 2 2004
Topher ZiCornell Xephyrus Java Simple Template Engine (JST) 0.9, 1.0, 1.1, 2.0, 2.1 (limited distro), 3.0 (public distro)	A Directory Traversal vulnerability exists because 'file-token' values may be overridden by URI parameters, which could let a malicious user obtain sensitive information. Upgrades available at: http://www.xephyrus.com/jest/ There is no exploit code required.	Xephyrus Java Simple Template Directory Traversal	Medium	Security Advis JST-001, August 16, 20
Whorl Limited JShop E-Commerce, Professional v3, JShop Server	A Cross-Site Scripting vulnerability exists in the 'page.php' script due to insufficient filtering of user-supplied input in the 'xPage' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	E-Commerce Suite Page.PHP Cross-Site Scripting	High	Indonesia Security Development Team Advisor August 22, 20

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listse or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
August 31, 2004	dlinkdown.c	No	Remote exploit that will change an IP address for the D-Link DCS-900 IP camera, due to the fact that it listens for a 62976/udp broad packet telling it what IP address to use without any authentication.
August 31, 2004	gc2boom.zip	No	Proof of concept exploit for the denial of service vulnerability in Ground Control II: Operation Exodus versions 1.0.0.7 and below.
August 31, 2004	gwee-1.36.tar.gz	N/A	Generic Web Exploitation Engine (gwee), is a small program designed to exploit input validation vulnerabilities in web scripts, such as Perl CGIs, PHP, etc. gwee is much like an exploit, except more general-purpose.
August 31, 2004	keeneTraversal102.txt	No	Proof of concept exploit for Keene Digital Media Server version 1.0.2 which is susceptible to a directory traversal attack due an input validation vulnerability
August 31, 2004	neb-citadel.c	Yes	Remote exploit for Citadel/UX versions 6.23 and below that makes use of the USER directive overflow vulnerability.
August 31, 2004	skl0g_v1.14.zip	N/A	skl0g is a keylogger for Windows. It runs invisibly, logs everything that is typed at the computer and saves them in log files according the date.
August 31, 2004	tcpick-0.1.24.tar.gz	N/A	tcpick is a textmode sniffer that can track TCP streams and saves the data captured in files or displays them in the terminal.
August 31, 2004	weplab-0.1.0-beta.tar.gz weplab-0.1.0-beta-win32_01.zip	N/A	Weplab is a tool to review the security of WEP encryption in wireless networks. Several attacks are available to help measure the effectiveness and minimum requirements for the network.
August 27, 2004	aircrack-1.3.tgz	N/A	Aircrack is an 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have bee gathered. It implements the standard FMS attack along with some optimizations, thus making the attack much faster compared to oth WEP cracking tools.
August 27, 2004	Codebase.gen	No	Code that exploits the Winamp skin remote code execution vulnerability.
August 27, 2004	gaucho140poc.cpp.txt	Yes	Proof of concept exploit that simulates a POP3 server which sends a specially crafted email to a vulnerable Gaucho email client, triggering an overflow and binding a shell on port 2001. Version 1.4 build 145 is susceptible.
August 27, 2004	winampExploit.txt	No	Proof of concept exploit that was found in the wild by k-otik.com that makes use of the Winamp vulnerability where insufficient restrictions on Winamp skin zip files (.wsz) allow a malicious attacker to place and execute arbitrary programs on a victim's system.
August 26, 2004	00045-08242004.txt	No	Proof of concept exploit for the denial of service and unauthorized system access vulnerabilities in Easy File Sharing webserver versi 1.25.
August 26, 2004	efswsdos.pl	No	Proof of concept exploit for the denial of service vulnerability in Easy File Sharing webserver version 1.25.
August 26, 2004	gallery-php.txt	Yes	PHP based exploit for Gallery versions 1.4.4 and below that makes use of an arbitrary file upload flaw.
August 26, 2004	gc2.tar	No	Proof of Concept exploit for the Ground Control II Remote Denial of Service vulnerability.
August 26, 2004	gmailSurf.txt	Yes	Proof of concept exploit for input validation vulnerability in Google's GMail system which allows users to surf anonymously.
August 26, 2004	md-xplv2.c	No	Script that exploits the Music Daemon Information Disclosure vulnerability.
August 26, 2004	networkEverywhere.txt	No	Proof of concept exploit for the script injection over DHCP vulnerability in NetworkEverywhere router Model NR041.
August 26, 2004	painkex.zip	No	Proof of concept exploit for Painkiller versions 1.3.1 and below that makes use of a memory corruption flaw.
August 26, 2004	PST_chpasswd_exp-v_b.c	Yes	Squirrelmail chpasswd local root bruteforce exploit.
August 26, 2004	RealVNC_dos.c	No	Proof of Concept exploit for the RealVNC Server Remote Denial of Service vulnerability.
August 26, 2004	webapp.traversal.txt	No	Proof of concept exploit the WebAPP vulnerabilities that could permit a directory traversal attack and the ability to retrieve the DES encrypted password hash of the administrator.
August 25, 2004	find_shell code	N/A	This shellcode scans the address space of the vulnerable process for a certain pattern. Once found it jumps into it. This assumes that remote buffer overflow target has limited buffer space and storing the bind shellcode in the buffer is difficult but storing it "somewhere" possible.
August 24, 2004	00042-08202004.txt	No	Proof of concept exploit for the BadBlue Webserver version 2.5 Denial of Service vulnerability.
August 24, 2004	AntiExploit-1.3b2.tar.gz	N/A	AntiExploit is an exploit scanner to detect local intruders. It scans for over 3900 suspicious files, has daily database updates, and will if a file is accessed. It uses the dazuko kernel module, which is also used by clamAV, Amavis, and other virus scanners.
August 24, 2004	axisFlaws.txt	No	Proof of concept exploit for multiple vulnerabilities in Axis versions 2100, 2110, 2120, 2420, and 2130 Network Camera along with the 2400 and 2401 Video Servers.
August 24, 2004	hafiye.txt	No	Proof of concept exploit for Hafiye 1.0 terminal escape sequence injection vulnerability that can result in a denial of service and remot root compromise.
August 24, 2004	musicDaemon.txt	No	Proof of concept exploit for the MusicDaemon versions 0.0.3 and prior remote Denial of Service and other vulnerabilities.
August 24, 2004	MyDMS.txt	Yes	Proof of concept exploit for the MyDNS SQL injection and directory traversal vulnerabilities.
August 24, 2004	qt_bmp_heap_overflow.c	Yes	Proof of concept exploit for the qt BMP parsing vulnerability in version 3.3.2.
August 24, 2004	qt_bmpslap.c	Yes	Heap overflow exploit for the qt BMP parsing vulnerability in version 3.3.2.
August 24, 2004	regmon_dos.c	No	A Proof of Concept exploit script for the Regmon Local Denial of Service vulnerability.
August 24, 2004	txt-rant.txt	N/A	Information about how Microsoft and Virus scanners fail to properly pay attention to .txt file extensions and how they can be used by attackers to fall into the background.
August 23, 2004	birdCahtDOSExploit.java	No	Exploit for the Bird Chat Remote Denial of Service vulnerability.
August 20, 2004	badblue_webserver_dos.pl	No	Proof of Concept exploit for the BadBlue Webserver Denial Of Service vulnerability.
August 20, 2004	xv_bmpslap.c	No	Script that exploits the xv vbmp.c Buffer Overflow vulnerability
August 19, 2004	malware.sp2.zip	No	Exploit for the Internet Explorer MHTML Content-Location Cross Security Domain Scripting vulnerability.
August 19, 2004	malware.sp2.zip	Yes	Exploit for the Internet Explorer MHTML Content-Location Cross Security Domain Scripting vulnerability.
August 19, 2004	merak527.txt	Yes	Script that exploits various vulnerabilities in the Merak Webmail server version 5.2.7.

			a few text-based databases, and optional Perl modules. It should run on almost every Unix variety except Solaris and NetBSD.
August 19, 2004	yapig-php.txt	No	PHP based exploit script for YaPiG 0.x.
August 18, 2004	gv-exploitv2.c	Yes	Script that exploits the local buffer overflow vulnerability in the gv postscript viewer.
August 18, 2004	Imailpwdump.cpp	Yes	Password decryption utility for the IpSwitch IMail Server versions 8.1 and prior.
August 18, 2004	ipd-dos.c	Yes	Proof of concept exploit for the IPD (Integrity Protection Driver) Denial of Service vulnerability.
August 18, 2004	playsms_sql.pl	No	Proof of Concept exploit for the PlaySMS SQL Input Validation vulnerability.
August 17, 2004	dnsspoof.zip	Yes	Utility that automates the DNS spoofing vulnerability in Microsoft Windows XP SP1. It generates a script file that launches the netwox application with correct parameters. It works with Windows and Linux.
August 17, 2004	xine_bof.c	Yes	Script that exploits the xine Buffer Overflow in Processing 'vcd' Identifiers Lets Remote Users Execute Arbitrary Code vulnerability.

[back to top]

Trends

- US-CERT Cyber Security Alert SA04- 243A: Security Improvements in Windows XP Service Pack 2. Windows XP Service Pack 2 is a major operating system update that contains a number of new security updates and features. Like other Microsoft Service Packs, Windows XP Service Pack 2 also includes previously released security fixes and other operating system updates. To help protect your Windows X computer from attacks and vulnerabilities, install Service Pack 2 using Windows Update or Automatic Updates. Service Pack 2 makes significant changes to improve the security of Windows XP, and these changes may have negative effects effects on some programs and Windows functionality. Before you install Service Pack 2, back up your important data and consult your computer manufacturer's web site information about Service Pack 2. Downloads are available at: http://www.microsoft.com/windowsxp/sp2/default.mspx. See US-CERT Advisory at: http://www.uscert.gov/cas/alerts/SA04- 243A.html

[back to top]

Viruses/Trojans

New Viruses / Trojans

Viruses or Trojans Considered to be a High Level of Threat

- Download.Ject: A new version of Download.Ject infects vulnerable systems with a Trojan horse and a keystroke logger. Unlike the original Download.Ject worm, the new worm generates pop-up advertisements to pornographic sites and changes the Web home page and the Internet Explorer search pane on infected systems. the attacks begin with instant messages sent to people using America Online's AOL Instant Messenger or ICQ instant messaging program inviting recipients to click on a link to a Web page.
- W64.Shruggle.1318: While not a high threat virus, W64.Shruggle.1318 is the first known virus to attack 64-bit Windows executables on AMD64 systems. This virus infects AMD64 Windows Portable Executa (PE) files.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This informa has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Compute Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variar that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
BKDR_SURILA.G		Trojan
CHM_PSYME.N		Compiled Help virus
Download.Ject.B		Trojan
Download.Ject.C		Trojan
Downloader.CDT		Trojan
Downloader-NV	Trj/Delf.AH Troj/Delf-DV TrojanDownloader.Win32.Delf.ch	Trojan
Downloader-NY	Adware.Quadro	Trojan
Downloader-OG		Trojan
Downloader-OL		Trojan: Adware Downloader
Exploit.HTML.Mht		HTML Exploit
Gaobot.AIR	W32/Gaobot.AIR.worm	Win32 Worm
HTML_MHTREDIR.V		HTML Virus
MhtRedir.S	Exploit/MhtRedir.S	Trojan
MyDoom.m.log	I-Worm.MyDoom.m.log	Win32 Worm
Netsnake		Trojan
Phish-BankFraud.eml		E-mail Scam
PWS-DoomTweak		Trojan: Password Stealer
PWSteal.Bancos.I		Trojan: Password Stealer
PWSteal.Bancos.J		Trojan: Password Stealer
PWSteal.Bancos.K	Troj/Banker-K	Trojan: Password Stealer
QDial27		Trojan: Dailer
Sasser.G	W32.Sasser.G W32/Sasser.G.worm W32/Sasser.worm.g Worm.Win32.Sasser.g Worm.Win32.Sasser.gen	Win32 Worm
StartPage.JL	targetsearch.info Trj/StartPage.JL	Trojan
Startpage-EU	Download.Ject2	Trojan
Tibick.A	W32.Tibick Win32.Tibick.A Win32/Tibick.A.Worm Worm.P2P.Tibick	Win32 Worm
Trivial.818		DOS Virus
Troj/Agent-BX	BackDoor.Agent.bx	Trojan
Troj/LeechPie-A		Trojan
Troj/LegMir-R	Trojan.PSW.Lmir.qj PWS-LegMir.dll PWSteal.Lemir.Gen	Trojan
Troj/Winflux-B	Backdoor.Win32.Flux.d TrojanSpy.Win32.Flux.a	Trojan
Trojan.Delsha	Delsha	Trojan
Trojan.Mitglieder.N	W32/Bagle.ak!proxy	Trojan
Trojan.Mitglieder.O		Trojan
Trojan.StartPage.H		Trojan
Trojan.Treb	Treb	Trojan
VBS.Voodoo.C	VBS.Voodoo.B	Visual Basic Script Virus

W32.Beagle.AP@mm	Beagle.AP WORM_BAGLE.AJ	Win32 Worm
W32.Lovgate.AO@mm	I-Worm.LovGate.ah Lovgate.AO	Win32 Worm
W32.Scane	Scane	Win32 Worm
W32.Spybot.DAZ	Backdoor.Rbot.gen	Win32 Worm
W32.Tiniresu		Win32 Worm
W32/Agobot-ME	Backdoor.Agobot.gen	Win32 Worm
W32/Agobot-ME	Backdoor.Agobot.gen	Win32 Worm
W32/Apler-A	Worm.Win32.Apler Win32/Apler.A W32.Gramos TROJ_RANCK.A	Win32 Worm
W32/Bagle-AJ	I-Worm.Bagle.am	Win32 Worm
W32/Forbot-E	WORM_SDBOT.SR Backdoor.Win32.Agent.cf	Win32 Worm
W32/Forbot-K	Backdoor.Win32.ForBot.k W32/Sdbot.worm.gen WORM_SDBOT.OU	Win32 Worm
W32/Forbot-L		Win32 Worm
W32/Rbot-GO	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-GP	Backdoor.Rbot.gen W32/Sdbot.worm.gen.n W32.Spybot.Worm	Win32 Worm
W32/Rbot-GR	Backdoor.Rbot.gen W32/Sdbot.worm.gen.g W32.Spybot.Worm	Win32 Worm
W32/Rbot-GS	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-GX	Backdoor.SdBot.ma Win32/Rbot.CP WORM_AGOBOT.LU	Win32 Worm
W32/Rbot-HB	Backdoor.Rbot.gen WORM_SDBOT.NP	Win32 Worm
W32/Rbot-HC	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-HE	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-HI	Backdoor.Rbot.gen W32/Sdbot.worm.gen.o	Win32 Worm
W32/Rbot-HO	Backdoor.Rbot.gen	Win32 Worm
W32/Sdbot-NO	Backdoor.SdBot.gen	Win32 Worm
W32/Sdbot-NQ	Backdoor.SdBot.gen WORM_RBOT.ID	Win32 Worm
W32/Sdbot-NR	Backdoor.IRCBot.gen WORM_IRCBOT.C W32/Sdbot.worm.gen.r virus	Win32 Worm
W32/Sdbot-OC	Worm.Win32.Donk.d WORM_SDBOT.SE	Win32 Worm
W32/Tzet-B	Worm.Win32.Tzet W32/Tzet.worm.e Win32/Tzet.A.dropper	Win32 Worm
W32/Wort-A		Win32 Worm
W32/Wukill-C	W32/Wukill.worm W32.Wullik@mm WORM_WUKILL.D	Win32 Worm
W64.Shruggle.1318	Win64.Shruggle.1318 W64/Shruggle W64_SHRUGGLE.A	Win64 Virus
Win32.Bagle.AH	Bagle.AH I-Worm.Bagle.am W32.Beagle.AP@mm W32/Bagle.AK@mm W32/Bagle.ar@MM Win32.Bagle.AH Win32/Bagle.AH.Worm	Win32 Worm
Win32.Bugbros.B	W32.Bugbros.B@mm W32/VB.CF@mm Win32/Bugbros.B.Worm	Win32 Worm
Win32.Gavvo	Backdoor.Win32.Surila.g	Win32 Worm
Win32.Glieder.D	I-Worm.Bagle.al W32.Beagle.AO@mm Win32/Bagle.AG.Downloader.Worm	Win32 Worm
Win32.Myss.CB	Spy-Tofger.gen.b Win32/Myss.Variant	Win32 Worm
WORM_REMADM.A	Backdoor.Win32.RA-based.c BKDR_REMADM.A	Win32 Worm
X97M.Ainesey.B		MS Excel Macro Virus
X97M.Ainesey.C		MS Excel Macro Virus
XF/NetSnake		MS Excel Virus

[back to top]